Monthly Research

OS X と iOS における脅威について

株式会社ＦＦＲＩ
http://www.ffri.jp

はじめに

- 近年では、Mac や iPhone, iPad の業務利用が増加しており、背景としては・・・
  - VMware などの仮想マシンや Boot Camp で Windows との共存が可能
  - Unix ベースの OS であり様々なコマンドラインユーティリティが標準で利用できるため、デザイン業務だけでなく、Web 系を中心に開発用端末としても利用しやすい
  - 標準のリモートワイプ機能や iPhone に対応した MDM ソリューションなどがあるため、企業が業務用モバイル端末として選択肢に入れている
    - 特に日本は世界的に見て iPhone ユーザーが多く、企業が BYOD を認めた場合、必然的に iPhone が業務利用される図式が成り立ちやすい
    - これまでの事例などから、Android よりもマルウェアが少ないと認識されている

- 2015年4月に開催された RSA Conference 2015 にて、OS X に搭載されている４つのセキュリティ機構(Gatekeeper, XProtect, App Sandbox, Code Signing)が容易に回避可能であることが発表された
  - また、現在販売されている Mac 向けのあらゆるセキュリティソフトで検知が不可能な攻撃手法が発表された

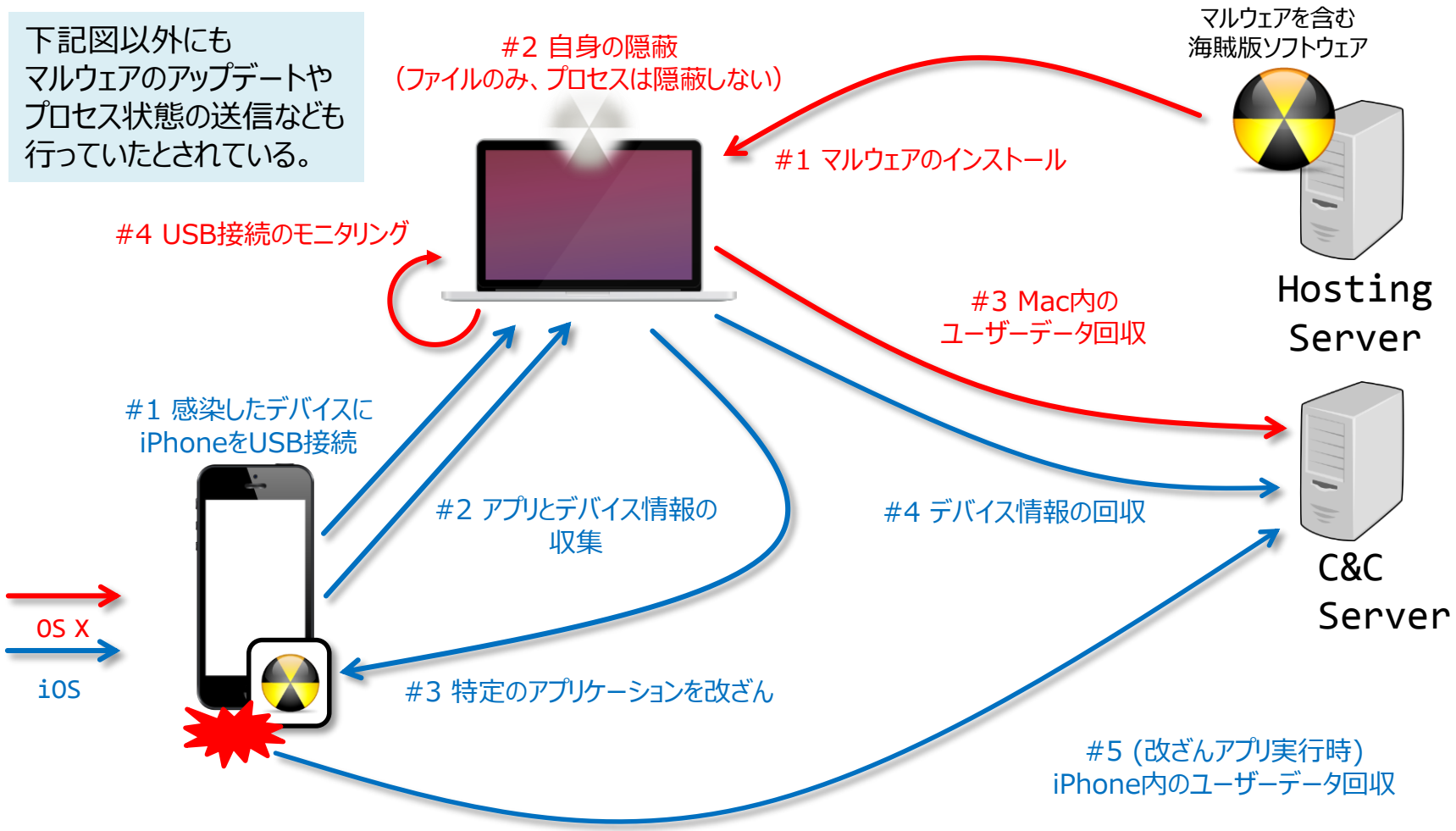
- これらの背景に基づいて、OS X/iOS における脅威の動向について調査した

マルウェア事例

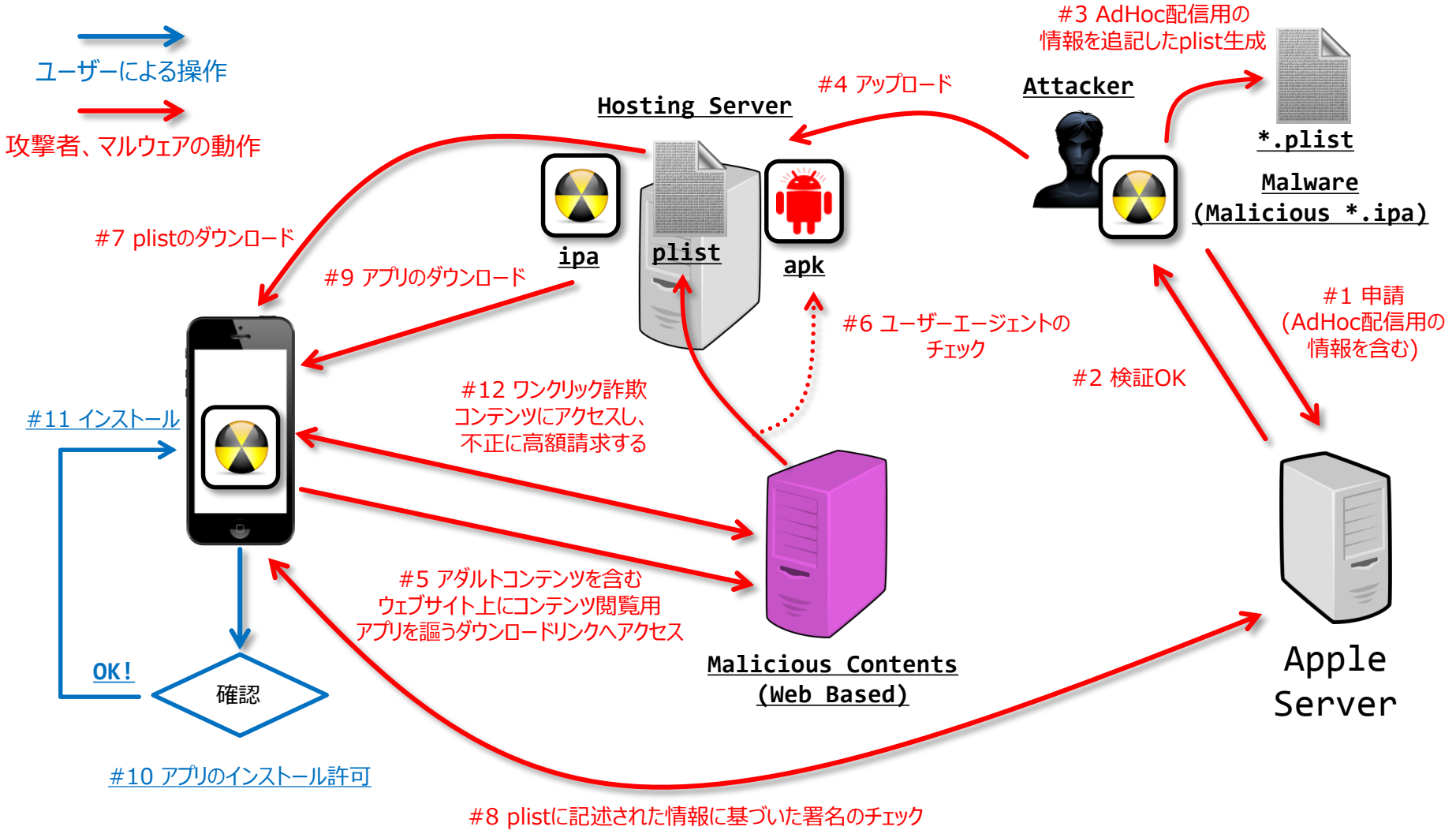
- [OSX/2014年] iWorm
  - 主に海賊版ソフトウェアに仕込まれており、インストールによって感染
  - ボット型マルウェアであり、攻撃者がソーシャルニュースサイト reditt.com に書き込む C&C サーバのアドレスとポートのリストを受信し、そこに接続して命令を受け取る
- [iOS/2014年] WireLurker
  - 主に海賊版ソフトウェアに仕込まれており、インストールによって感染
  - Windows および OS X を媒介とし、同期処理を悪用して iPhone に感染
  - 電話帳の情報を C&C サーバに送信する機能を持っているとされる
- [iOS/2015年] ワンクリック詐欺アプリ
  - 企業向けの開発者プログラム(iOS Developer Enterprise Program)を悪用することで AppStore 以外でアプリを配布、感染
  - Android などで一般的な詐欺アプリ同様にウェブサーバー側に悪意のあるコンテンツが用意されているのが特徴

WireLurker の感染フロー

下記図以外にも
マルウェアのアップデートや
プロセス状態の送信なども
行っていたとされている。



ワンクリック詐欺アプリの感染フロー

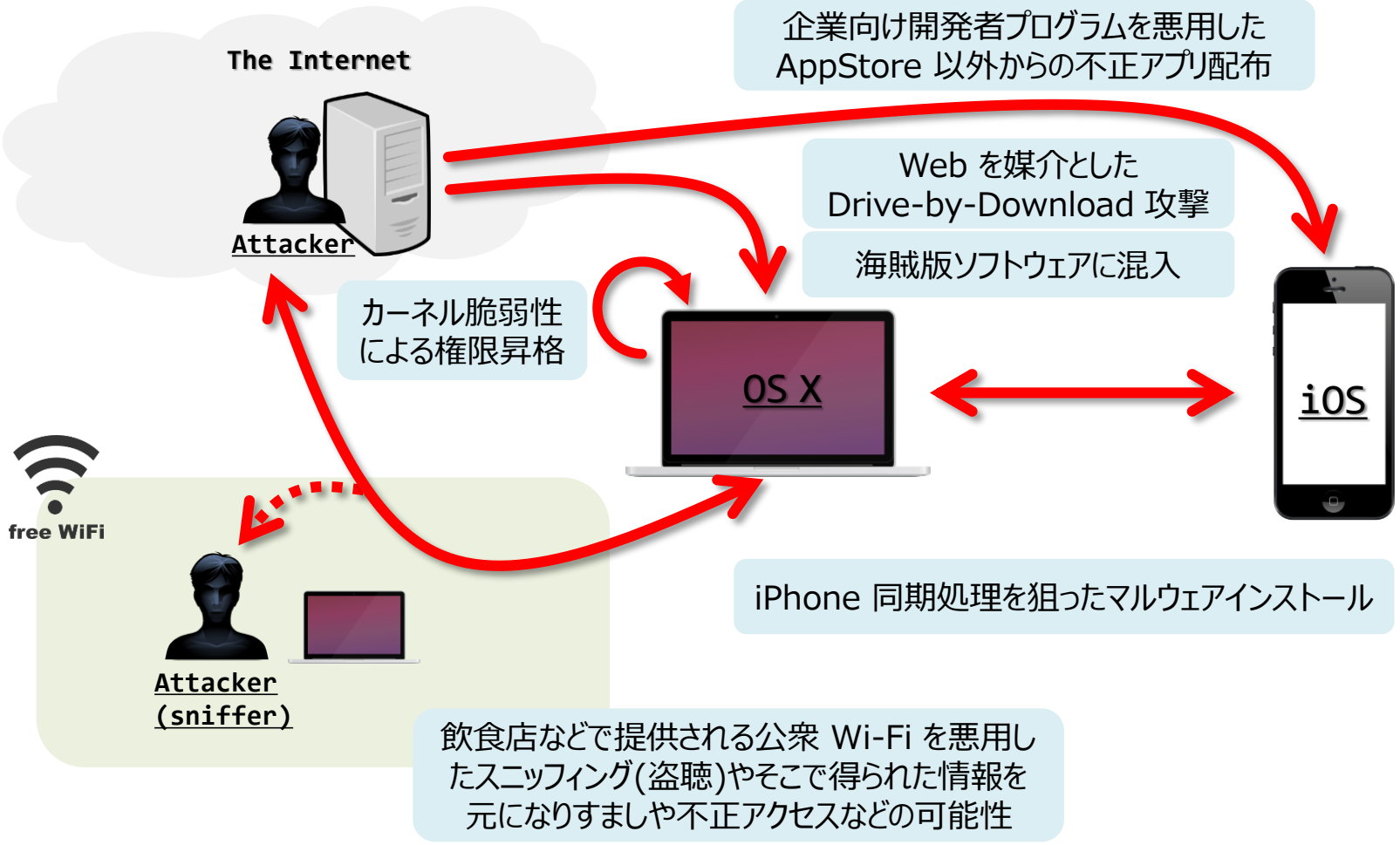


脆弱性事例

- [OS X/iOS] メッセンジャーアプリの脆弱性
  - 2015年5月に報告された特定のメッセージを受け取ると、アプリもしくは OS がクラッシュして再起動する脆弱性(CVE-2015-1157)
  - 受け取った場合、以降はメッセンジャーアプリが起動できなくなる
  - iOS 8.4 で修正済み

- [OS X/iOS] クロスアプリケーションリソースアクセスの脆弱性
  - 2015年6月に報告された、アプリ間認証に関する脆弱性 今までもアプリ間認証に関する脆弱性はいくつか見つかっているが、この脆弱性が悪用された場合、パスワード情報など任意のリソース情報がマルウェアによって奪取される恐れがある
  - Apple によれば、サーバーサイドのセキュリティアップデートを実施することで、問題のあるアプリをストアから排除できるようにしたとのこと

想定される主なサイバー攻撃・感染経路



まとめ

- 以前は、OS X/iOS はマルウェアやサイバー攻撃の被害にあう可能性は普及率や限定されたアプリケーションの配布経路などを理由に低いとされてきた

- しかし、近年では OS X/iOS 向けのマルウェアが増加傾向にあり、数は Windows 程では無いが、攻撃者は Windows 同様に攻撃対象として認識していると推測できる
  - その結果、前述の「想定される主なサイバー攻撃・感染経路」に示すとおり、攻撃経路の多様化や、Mac/iPhone(iPad)独自ともいえる攻撃手法も登場してきている

- 最後に、 OS X/iOS をサイバー攻撃やマルウェアの脅威から守るための設定などについて紹介する
  - ターゲットは OS X 10.10.x (Yosemite)、iOS 8.x
  - ただし、これらは最低限の対策の一例であり、未知の脅威を確実に防御することを保障するものではない

Mac/iPhoneですぐ出来るセキュリティ対策

すぐ出来る Mac のセキュリティ対策 #1

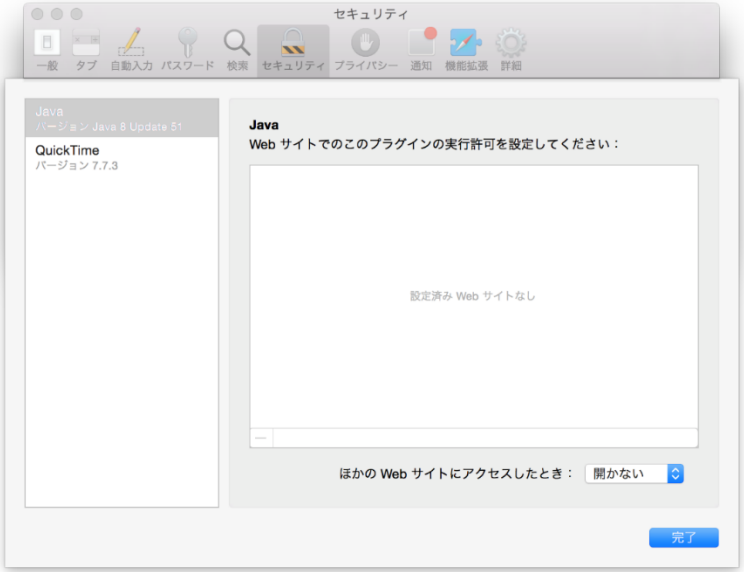
1．セキュリティアップデートを自動的にインストールする

- セキュリティアップデートによって脆弱性が修正されるため、**脆弱性攻撃対策として Windows 同様に常に最新の状態にしておく**ことを推奨
- OS 以外のアプリケーションについても、チェックを入れておくことを推奨
  - 「～をインストール」にチェックしない場合は、アップデート通知のみが行われる

すぐ出来る Mac のセキュリティ対策 #2

2．ブラウザの Java プラグインを無効化する

- Mac の**マルウェア感染の多くは、Java の脆弱性を突いたウェブ感染**といわれている
- そのため、Java プラグインは、無効化もしくは必ず使用有無を確認する設定としておくことを推奨する
  - Yosemite は標準で Java はインストールされていないため、ここで Java の項目が見えない場合は、特に設定は不要



すぐ出来る Mac のセキュリティ対策 #3

3．ファイアーウォールの有効化

- **外部からの不正アクセスを防ぐ**為に、ファイアーウォールを有効化を推奨

すぐ出来る Mac のセキュリティ対策 #4

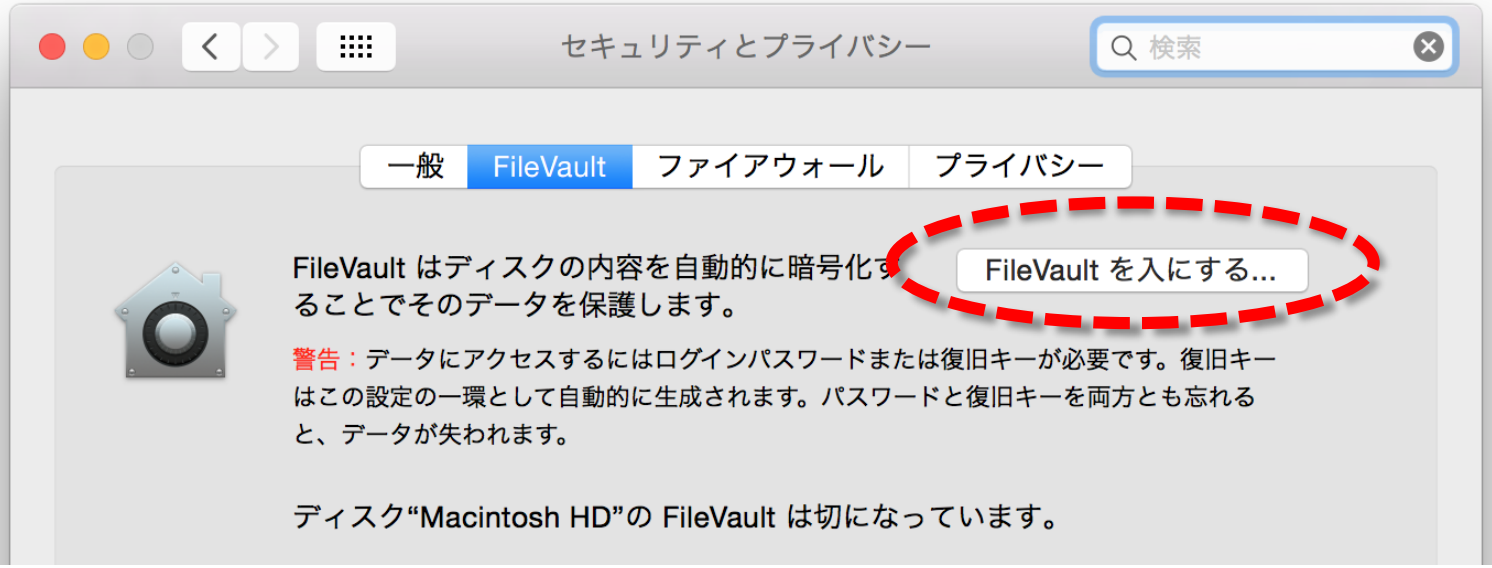
4．Finder の設定

- Finder では、「拡張子の表示」、「ゴミ箱を確実に空にする」などの設定が可能
- 特に、Finder はデフォルトで拡張子の表示を行わない設定となっていることから、**アイコン偽装された実行ファイルなどの怪しいファイルを見分ける為**に表示設定にしておくことを推奨
- これは、Windows クライアントに対して**添付メールを送る際に誤って不審なファイルを添付しない為**にも重要である

すぐ出来る Mac のセキュリティ対策 #5

5．ファイルの暗号化（FileVault）を有効化

- 起動ディスクの暗号化を行うことで、**紛失や盗難時におけるデータの流出を防ぐことが期待**できる



すぐ出来る Mac のセキュリティ対策 #6

6．パスワードによるスクリーンロック

- ファイルの暗号化同様、**紛失や盗難時におけるデータの流出を防止する効果が期待**できる

すぐ出来る Mac のセキュリティ対策 #7

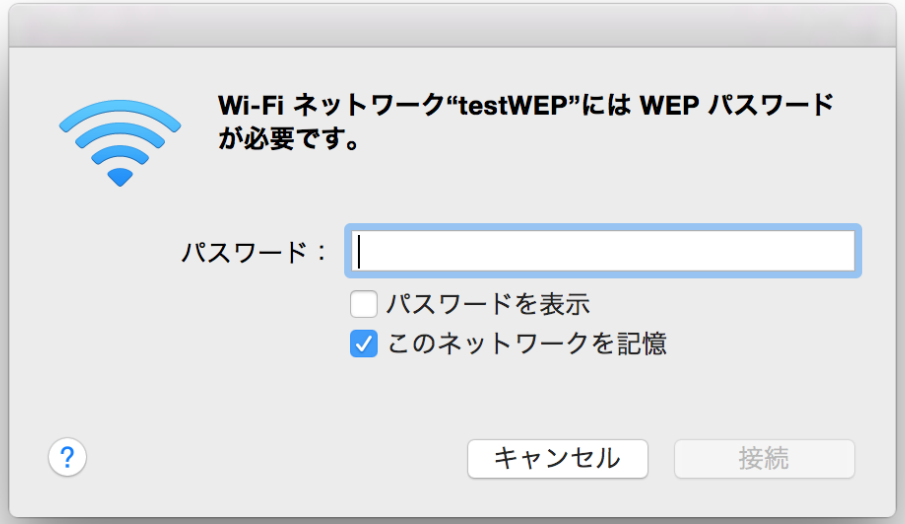
7．ゲストユーザーを有効にしない

- ゲストユーザーを無効化は**攻撃者の侵入経路を減らす効果**が期待できる（ゲストログイン後に権限昇格など）

すぐ出来る Mac のセキュリティ対策 #8

8．無線 LAN 接続に強度な暗号を使用する

- 無線 LAN を使用する際は**暗号化を必ず行い、暗号化方式は WEP, WPA-PSK(TKIP) 以外の方式を使う**
- 弱い暗号は解析ツールを用いることで容易に解読が出来てしまうため。
  （実際に解析ツールでパスワードクラックを行い踏み台にした事件も発生している）



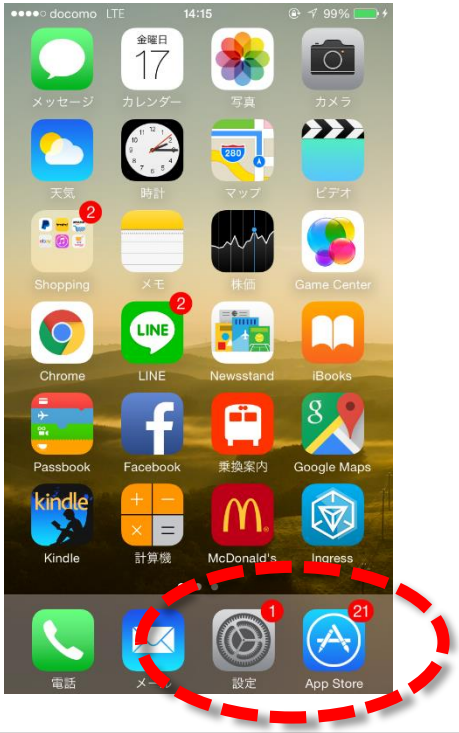
すぐ出来る Mac のセキュリティ対策 #9

9．Mac を探す機能の有効化

- iCloud と連携することで、自身の位置が特定可能な条件下において、**紛失や盗難された Mac の位置を検索することが可能**となる
- この他、**” 音を鳴らす”、”端末をロックして任意のメッセージを表示する”、“ワイプする”などの機能も利用可能**である

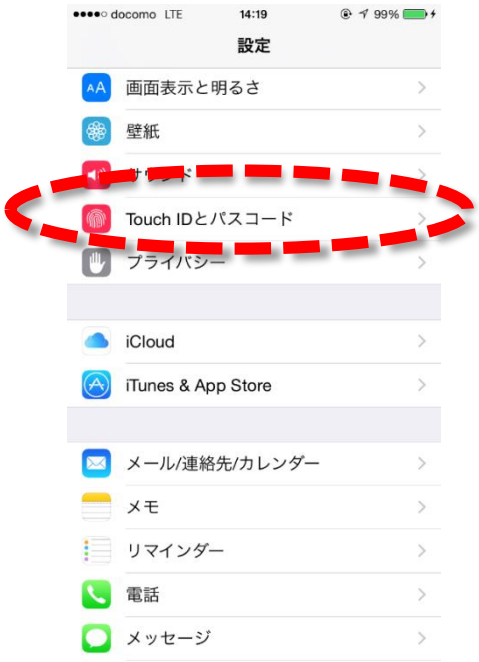
すぐ出来る iPhone のセキュリティ対策 #1

- アップデートの確認と適用
  - iOS は、OS のアップデートにセキュリティアップデートが含まれるため、古いバージョンを使い続けている場合、脆弱性が未修正の状態となり、脆弱性攻撃を受けるリスクがある。



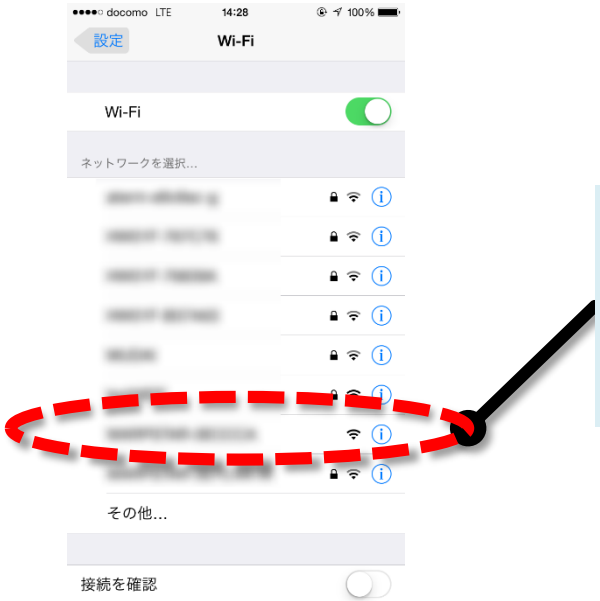
すぐ出来る iPhone のセキュリティ対策 #2

- Touch ID/パスコードによるスクリーンロックの有効化
  - **紛失や盗難被害にあった場合に、情報漏えいを防ぐ効果が期待**できる
  - 簡単なパスコードをオフにすることで、より複雑なパスワードを設定することが可能



すぐ出来る iPhone のセキュリティ対策 #3

- 無線 LAN 接続に強度な暗号を使用する
  - Mac 同様に、無線通信を行う場合の暗号化方式は、WEP, WPA-PSK(TKIP) 以外を推奨する
  - モバイルデバイスで SNS などを更新する際に、脆弱な暗号方式で通信をしていると、なりすまし等の被害にあう可能性がある



パスワードが不要なアクセスポイントに対しても不用意に接続しない
（**暗号化されないためリスクが高い**）

すぐ出来る iPhone のセキュリティ対策 #4

- 外部の PC にむやみに接続せず、接続しても信頼しない
  - 前出のスライドに記載した **WireLurker は仕組み上 iPhone を感染端末に接続した上で、感染デバイスとの通信をユーザーが許可する必要**がある。
  - そのため、信用できない外部の PC に接続する場合は該当 PC を信頼するべきでは無い。

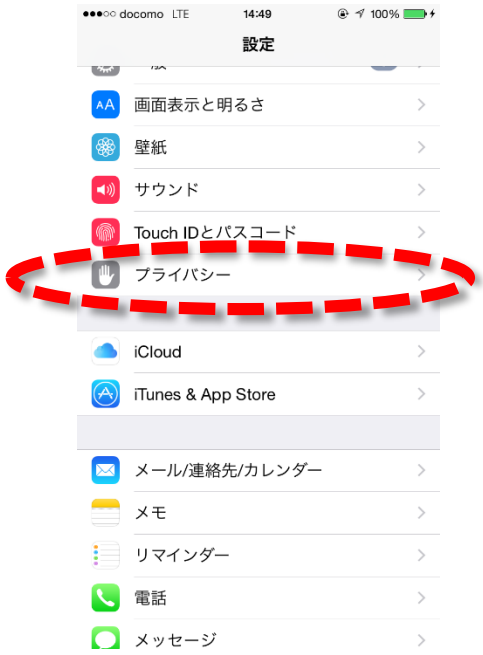
- 信頼できる開発元以外からのアプリはインストール・実行しない
  - ワンクリック詐欺アプリは**アプリケーションのインストールと実行時に、ユーザーに必ず確認**を行うため、AppStore や自身が所属する企業以外の信頼できない開発元からはインストール、実行するべきではない

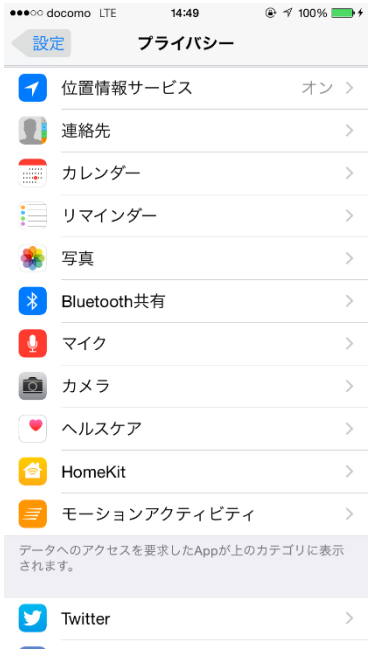
すぐ出来る iPhone のセキュリティ対策 #5

- iPhone を探す機能とバックアップの有効化
  - Mac 同様に、iCloud と連携して iPhone や iPad などのデバイスをウェブ上から探すことが出来る
  - 端末を紛失してしまった場合にiCloud上のバックアップデータから復元することも可能

すぐ出来る iPhone のセキュリティ対策 #6

- プライバシー設定の再確認
  - 位置情報サービスなど、アプリケーション毎に要求される機能の許可設定することが可能
  - プライバシー設定を確認し、端末にインストールされているアプリケーション毎が要求している機能やその利用状況を改めてチェックする





すぐ出来る iPhone のセキュリティ対策 #7

- 不審プロファイルがインストールされていないか確認する
  - 不審な企業によるプロファイル設定や身に覚えの無いプロファイル設定を削除する
  - 不正なプロファイルによって、悪意のあるアクセスポイントや VPN 設定が行われてしまい、通信を盗聴される可能性がある

参考情報

- Malware Persistence on OS X Yosemite
  - https://www.rsaconference.com/writable/presentations/file_upload/ht-r03-malware-persistence-on-os-x-yosemite_final.pdf
- WIRELURKER: A New Era in iOS and OS X Malware
  - https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
- iOS用アプリのAdHoc版を作る（Xcode）
  - http://mushikago.com/i/?p=2083
- Japanese one-click fraudsters target iOS users with malicious app delivered over the air
  - http://www.symantec.com/connect/blogs/japanese-one-click-fraudsters-target-ios-users-malicious-app-delivered-over-air
- Unauthorized Cross-App Resource Access on MAC OS X and iOS
  - https://drive.google.com/file/d/0BxxXk1d3yyuZOFlsdkNMSGswSGs/view?pli=1
- Serious OS X and iOS flaws let hackers steal keychain, 1Password contents
  - http://arstechnica.com/security/2015/06/serious-os-x-and-ios-flaws-let-hackers-steal-keychain-1password-contents/
- iPhone text message bug can crash Apple Watch, iPad and Mac too
  - http://www.theguardian.com/technology/2015/may/28/iphone-text-message-bug-crash-apple-watch-ipad-mac
- Malicious Profiles – The Sleeping Giant of iOS Security
  - https://www.skycure.com/blog/malicious-profiles-the-sleeping-giant-of-ios-security/
- NETMARKETSHARE
  - http://www.netmarketshare.com/
- openclipart
  - https://openclipart.org/share

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research